

KRIPTOGRAFIJA

zadaca 6.05

1. Zadan je broj $n = 2722481$. Nađite dvije baze b_1 i b_2 takve da je $(b_i, n) = 1$, $b_i \not\equiv \pm 1 \pmod{n}$ za $i = 1, 2$, te da je n pseudoprost broj u bazi b_1 , a da n nije pseudoprost broj u bazi b_2 .
2. Nađite neki jaki pseudoprosti broj n u bazi $b = 199$.
3. Metodom verižnog razlomka faktorizirajte broj

$$n = 10123.$$